Listing of Claims:

1. (previously presented) A method for securing information comprising:

receiving encrypted information from a sender for transmission to at least one intended recipient and receiving an encrypted secret key encrypted using a public key associated with a secure distribution server;

decrypting the encrypted secret key to produce a decrypted secret key;

obtaining a corresponding public key of the at least one intended recipient;

encrypting the decrypted secret key for the at least one intended recipient using a corresponding public key to produce at least one recipient specific secure secret key; and

forwarding the encrypted information sent by the sender and at least one recipient specific secure secret key for the at least one intended recipient.

2. (previously presented) The method of claim 1 including determining a plurality of intended recipients and retrieving corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key.

3. (original) The method of claim 1 wherein the step of encrypting the decrypted secret key with a corresponding public key of the at least one intended recipient includes encrypting a copy of the decrypted secret key for each intended recipient with a corresponding recipient public key.

4. (original) The method of claim 1 including the steps of: encrypting information with the secret key to produce the encrypted information, encrypting the secret key with a public key associated with the secure distribution server to produce the encrypted

secret key, and sending the encrypted information and the encrypted secret key to the secure distribution server.

5. (original) The method of claim 4 wherein encrypting the secret key includes encrypting the secret key using a public key for each of a plurality of secure distribution servers to produce a plurality of secure distribution server specific encrypted secret keys.

6. (previously presented) The method of claim 4 including storing the encrypted information in an encrypted form locally on a device that performed the step of encrypting information with the secret key.

7. (previously presented) The method of claim 4 further including the step of encrypting the secret key, by a sending device, with a public key associated with at least one of a user of the sending device and the sending device.

8. (previously presented) The method of claim 1 including the step of digitally signing the information using a private signing key associated with at least one of a user of a sending device and the sending device.

9. (original) The method of claim 1 further including the step of receiving the encrypted information and the encrypted secret key and forwarding the encrypted information and the encrypted secret key to the secure distribution server without decrypting the encrypted secret key.

10. (original) The method of claim 1 including the step of determining, by the secure distribution server, if the encrypted information needs to be sent to other entities, if so, encrypting the decrypted secret key using a public key associated with each of the additional entities.

11. (previously presented) The method of claim 1 including the steps of: encrypting the decrypted secret key using a public key associated with a content scanning device; sending the encrypted information and the encrypted secret key to the content scanning device; receiving a result back from the content scanning device, forwarding the encrypted information based on the result sent by the content scanning device and based on at least one recipient specific secure secret key for at least one intended recipient.

12. (original) The method of claim 2 wherein retrieving the corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key includes obtaining the corresponding public keys from at least one of: a certificate retrieval and validation service, an LDAP lookup and a certificate directory lookup.

13. (previously presented) The method of claim 1 including the steps of: encrypting information with a secret key to produce the encrypted information offline, encrypting the secret key with a public key associated with the secure distribution server to produce the encrypted secret key offline, and during an online session, sending the encrypted information and the encrypted secret key to the secure distribution server.

14. (original) The method of claim 1 including sending the encrypted information to a time stamper and receiving a time stamped result prior to forwarding the encrypted

information and the at least one recipient specific secure secret key for the at least one corresponding intended recipient.

15. (previously presented) A method for securing information comprising:

receiving, by a secure distribution server, encrypted information for transmission to a plurality of intended recipients and an encrypted secret key encrypted using a public key associated with the secure distribution server;

decrypting, by the secure distribution server, the encrypted secret key to produce a decrypted secret key;

obtaining, by the secure distribution server, a corresponding public key of at least one intended recipient;

encrypting, by the secure distribution server, the decrypted secret key for the at least one intended recipient using a corresponding public key of the recipient to produce a recipient specific secure secret key; and

forwarding, by the secure distribution server, the encrypted information and the recipient specific secure secret key for a corresponding intended recipient.

16. (previously presented) The method of claim 15 including determining a plurality of intended recipients and retrieving corresponding public keys of the plurality of intended recipients for encrypting the secret key.

17. (original) The method of claim 16 wherein the step of encrypting includes encrypting a copy of the decrypted secret key for each intended recipient with a corresponding recipient public key.

18. (previously presented) A network element comprising:

means for decrypting a received encrypted secret key encrypted using a public key associated with the network element to produce a decrypted secret key;

means, operatively coupled to the means for decrypting, for obtaining a corresponding public key of at least one intended recipient;

means, operatively coupled to the means for obtaining, for encrypting the decrypted secret key for the at least one intended recipient using a corresponding public key to produce a recipient specific secure secret key; and

means for forwarding the encrypted information sent by a sender and for forwarding at least one recipient specific secure secret key for at least one corresponding intended recipient.

19. (original) The network element of claim 18 wherein the means for obtaining retrieves corresponding public keys of a plurality of intended recipients for encrypting the decrypted secret key from at least one of: a certificate retrieval and validation service, an LDAP lookup and a certificate directory lookup.

20. (previously presented) A storage medium comprising:

memory containing executable instructions that when read by one or more processing devices, causes the one or more processing devices to:

receive encrypted information from a sender for transmission to at least one intended recipient and receive an encrypted secret key encrypted using a public key associated with a secure distribution server;

decrypt the encrypted secret key to produce a decrypted secret key;

obtain a corresponding public key of the at least one intended recipient;

encrypting the decrypted secret key for the at least one intended recipients using a corresponding public key to produce a recipient specific secure secret key; and

forward the encrypted information sent by the sender and forward at least one recipient specific secure secret key for the at least one intended recipient.

21. (previously presented) The storage medium of claim 20 including memory containing executable instructions that when read by the one or more processing devices causes the one or more processing devices to:

determine a plurality of intended recipients and retrieve corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key.

22. (original) The storage medium of claim 20 including memory containing executable instructions that when read by the one or more processing devices causes the one or more processing devices to encrypt a copy of the decrypted secret key for each intended recipient with a corresponding recipient public key.

23. (previously presented) The storage medium of claim 20 including memory containing executable instructions that when read by the one or more processing devices causes the one or more processing devices to determine if the encrypted information needs to be sent to other entities, if so, encrypting the decrypted secret key using a public key associated with each of the other entities.

24. (previously presented) A secure communication system comprising:

at least one sender that encrypts information with a secret key to produce encrypted information, encrypts the secret key with a public key associated with a network element to

produce an encrypted secret key, and during an online session, sends the encrypted information and the encrypted secret key to the network element;

at least one intended recipient;

at least one network element, operatively coupled to the sender and to the at least one intended recipient, including:

means for decrypting the received encrypted secret key encrypted using a public key associated with the network element to produce a decrypted secret key;

means, operatively coupled to the means for decrypting, for obtaining a corresponding public key of the at least one intended recipient;

means, operatively coupled to the means for obtaining, for encrypting the decrypted secret key for the at least one intended recipient using a corresponding public key to produce at least one recipient specific secure secret key; and

means for forwarding the encrypted information sent by the sender and forwarding at least one recipient specific secure secret key for at least one intended recipient.

25. (previously presented) The system of claim 24 wherein a sender encrypts information with the secret key to produce the encrypted information offline, encrypts the secret key with a public key associated with the network element to produce the encrypted secret key offline, and during an online session, sends the encrypted information and the encrypted secret key to the network element.

26. (previously presented) The system of claim 24 wherein the means for obtaining retrieves corresponding public keys of a plurality of intended recipients for encrypting the decrypted secret key from at least one of: a certificate retrieval and validation service, an LDAP lookup and a certificate directory lookup.

27. (previously presented) The system of claim 24 wherein the network element encrypts the decrypted secret key using a public key associated with a content scanning device; sends the encrypted information and sends the encrypted secret key to the content scanning device; receives a result back from the content scanning device, and forwards the encrypted information based on the result sent by the content scanning device and based on at least one recipient specific secure secret key for at least one intended recipient.